Troubleshooting WLANs

Tips and tricks with practical examples

by Gregor Vucajnk, Knowledge Services at Aerohive Networks
email: gvucajnk(at)aerohive.com, twitter: @GregorVucajnk

Get a free Aerohive AP/management

General International/Freeval AP webinar page:

http://www.aerohive.com/news-events/international-webinars

Registration page of the event held in Dutch language:

http://info.aerohive.com/June-simplified-wireless-Registration-Landing-Page-NL.html

“Troubleshooting is more of an art form than exact science.”

– The Internet

AGENDA

- Troubleshooting strategy.
- Basic troubleshooting methodology.
- Practical examples with commentary.

1. TROUBLESHOOTING STRATEGY

Aerohive
NETWORKS

Aerohive
NETWORKS
THE AVENGERS
Spigot

Dilbert

40 years of age
IT generalist
Babysits the rest of the IT team (usually junior members)

Source: www.dilbert.com

3. Basic Troubleshooting methodology

- Identifying the issue
- Recreate problem
- Locate and isolate the cause
- Formulate a plan of solving the problem
- Implement the plan
- Test to very the problem is resolved
- **Document** the problem and the solution
- Provide feedback to user

RINSE
AND
REPEAT

3. Practical examples

802.11 passive discovery

- Client devices can learn about the netw
  beacon frames. Beacon fra
  services. It con
  als
  ind
- By c
  subje

What to look for:

Beacon frames carry several important information. When troubleshooting Capabilities information (0x0511) and essentially all the Tags under Tag parameters. But remember, the capture is an interpretation of the capturing device. Can be deceiving.

802.

(wlan.fc.type_subtype eq 8)

802.11 active

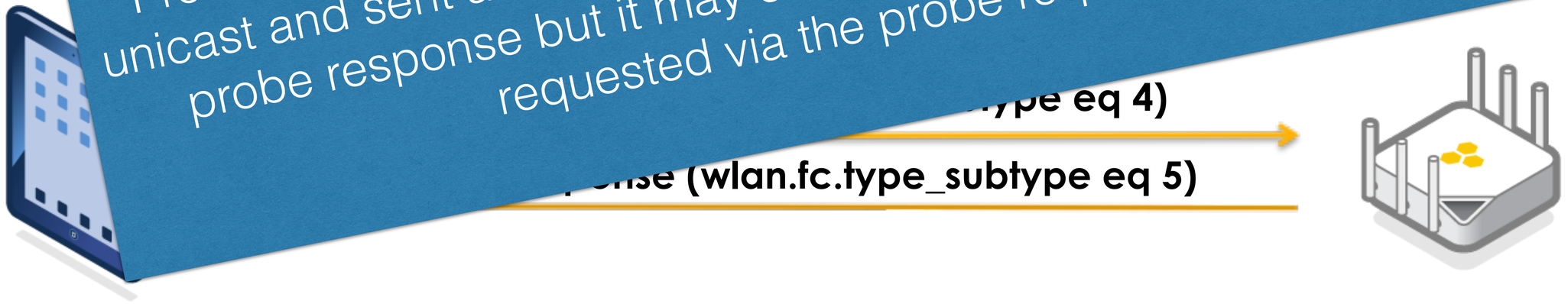
- Client devic… …ests
(… …s that
i… …tion
Q… …d,
ex…

- Tim…
imp…

What to look for:

Probe request is usually a broadcast frame. It contains the capabilities of the device and also may contain additional info about the device (device mode, manufacturer, etc). Probe request also says a lot on end client device roaming behaviour as the device hops channels all the time looking for other connections.

Probe response is very similar to beacon frame in structure. It is unicast and sent at the lowest common rate. There is no TIM field in probe response but it may contain RIE element that a station requested via the probe request



802.11 authentication

- 802.11 authentication should not be confused with [illegible]k authentication. It is a simple two fram[illegible]en the end client device and the AP [illegible]t device saying to th[illegible]n see you too

Where it brakes:

802.11 authentication should always work. However the exchange can be broken if MAC filtering is implemented at a SSID configuration level.

8[illegible]n request (wlan.fc.type_subtype eq 11)

802.11 authentication response (wlan.fc.type_subtype eq 11)

802.11 asso

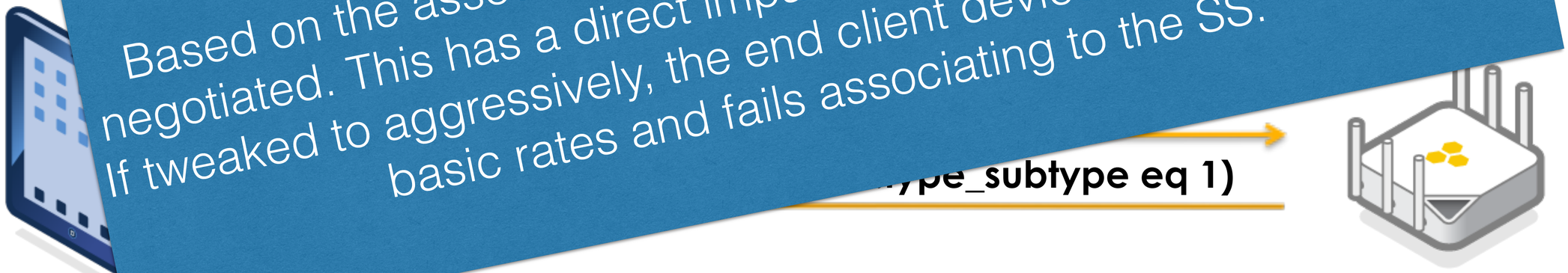
- 802.11
  - S
  - A
  - co
  - fra

se

What to look for:

Association phase sets up the requirements for network authentication (PSK, PPSK, 802.1X). If AP is overloaded (or the configuration is set to limit the amount of associations), the AP may reject client associations. There is also an impact from band-steering and load balancing that can affect the call flow.

Based on the association phase, the basic (mandatory) rates are negotiated. This has a direct impact on the overall network capacity. If tweaked to aggressively, the end client device may not support the basic rates and fails associating to the SS.



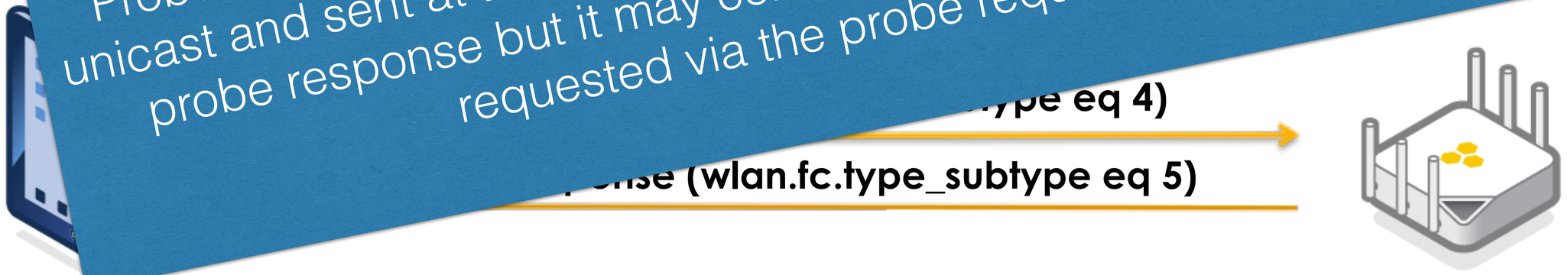
802.11 active

- Client device
- T
im

What to look for:

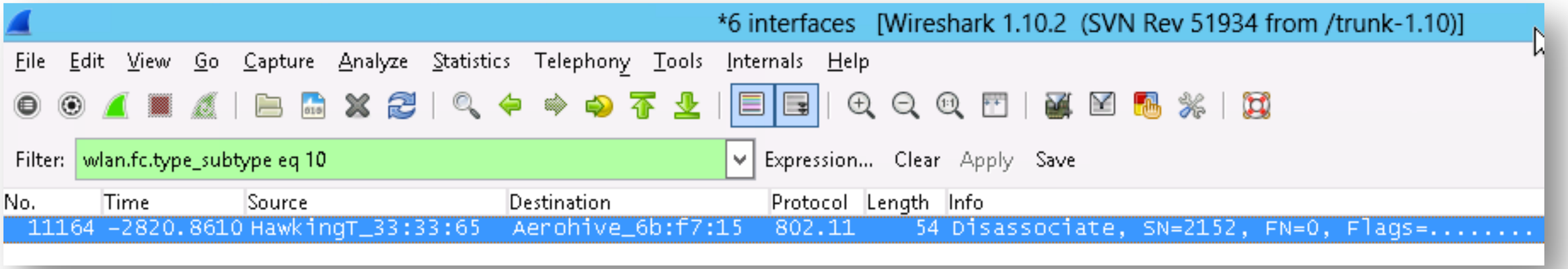
Probe request is usually a broadcast frame. It contains the capabilities of the device and also may contain additional info about the device (device mode, manufacturer, etc). Probe request also says a lot on end client device roaming behaviour as the device hops channels all the time looking for other connections.

Probe response is very similar to beacon frame in structure. It is unicast and sent at the lowest common rate. There is no TIM field in probe response but it may contain RIE element that a station requested via the probe request



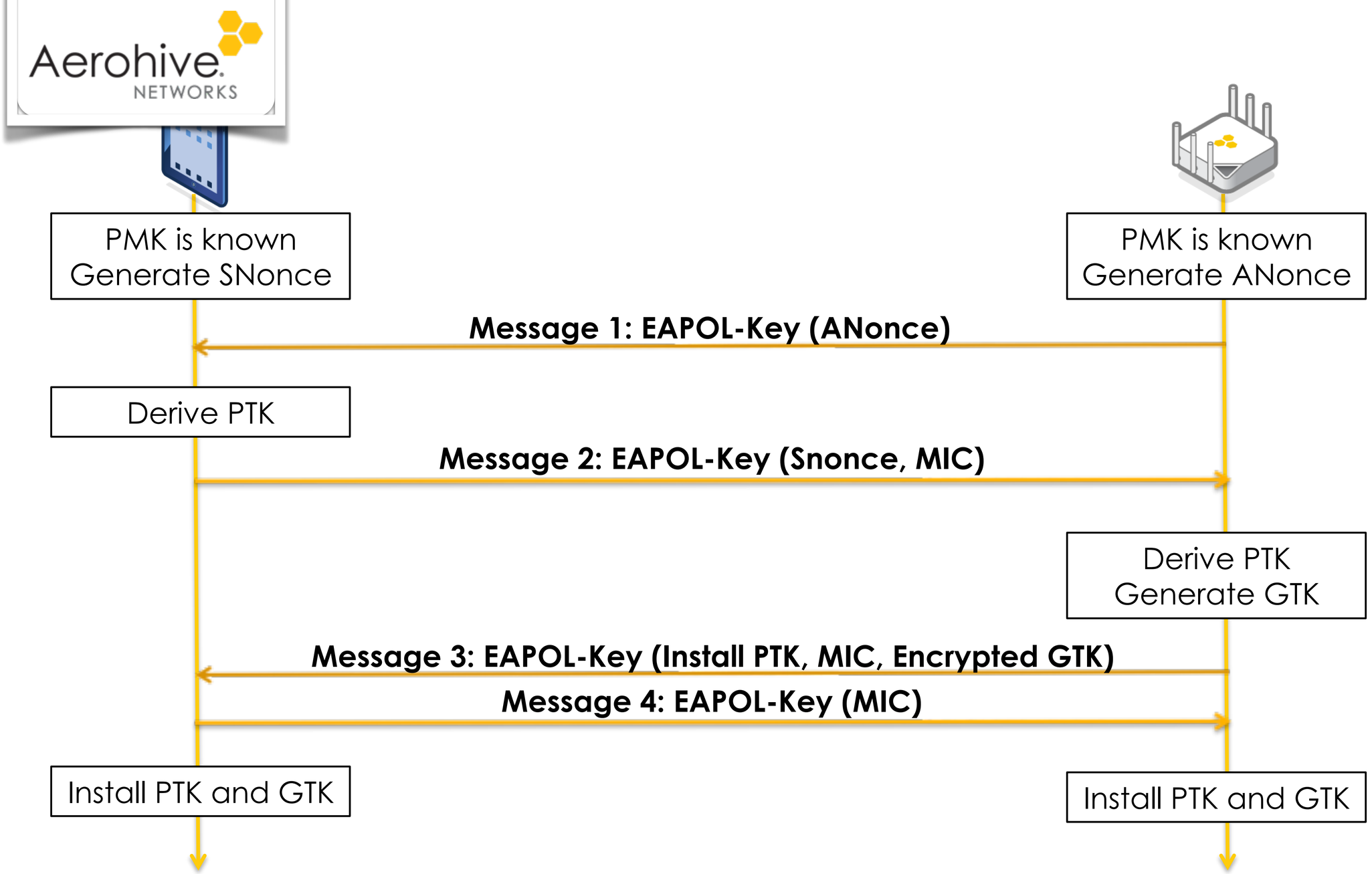
Additional management frames

- Reassociation request (wlan.fc.type_subtype eq 2) already a part of ESS and roaming to new AP
- Reassociation reponse (wlan.fc.type_subtype eq 3) similar to association but when roaming within ESS
- Diassociation (wlan.fc.type_subtype eq 10) (used in roaming to terminate connection)
- Deauthentication (wlan.fc.type_subtype eq 12) sent when all communication is terminated, ie, when the AP is rebooting).


*6 interfaces [Wireshark 1.10.2 (SVN Rev 51934 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: wlan.fc.type_subtype eq 10
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
11164 -2820.8610 HawkingT_33:33:65 Aerohive_6b:f7:15 802.11 54 Disassociate, SN=2152, FN=0, Flags=.....

4-way handshake

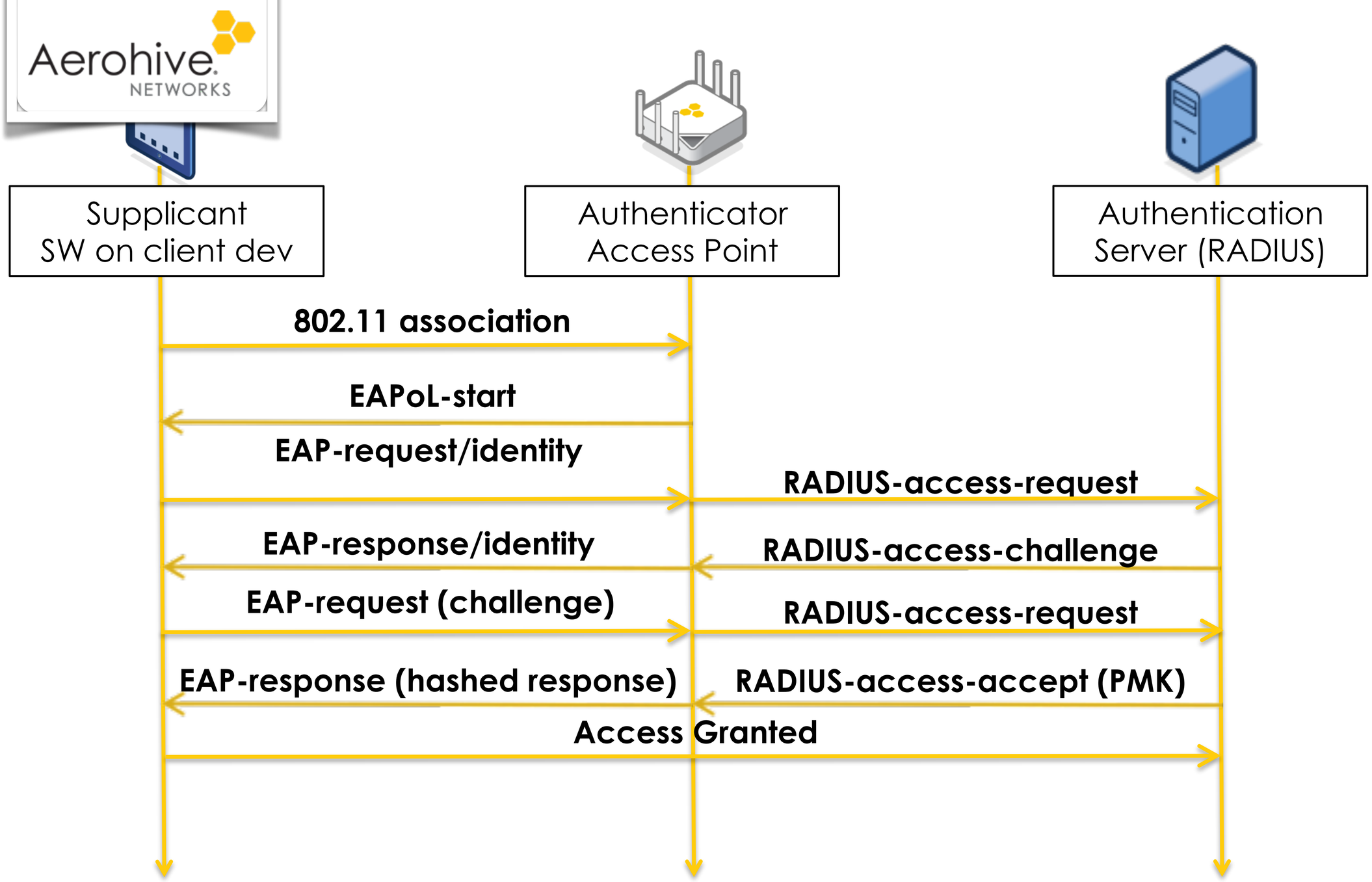
- Process by the source key material is turned in encryption material to encrypt our communication.
- It is done for EVERY* WPA(2) association and reasocciation (there is a slight difference when using 802.11r).
- Directly follows association phase for WPA(2)-Personal.
- Follows full EAP authentication for WPA(2)-Enterprise.
- Consists of four unicast frames.
- Only upon successfully completing the 4-way handshake is the traffic from the client device allowed to the network past the AP.


Aerohive
NETWORKS
PMK is known
Generate SNonce
PMK is known
Generate ANonce
Message 1: EAPOL-Key (ANonce)
Derive PTK
Message 2: EAPOL-Key (Snonce, MIC)
Derive PTK
Generate GTK
Message 3: EAPOL-Key (Install PTK, MIC, Encrypted GTK)
Message 4: EAPOL-Key (MIC)
Install PTK and GTK
Install PTK and GTK

4-way handshake

- After Message1 (1/4 is sent) -> Driv… …te driver.
- After Mess… …with PPSK.
- After Me… …Driver issue. Reboot, update driver.
- After Message 4 (4/4 is sent) -> It becomes a network issue. Check DHCP, DNS, FW, VLANs, etc.

Hint: bad RF connectivity can exuberate any higher level communication issues. Make sure L1 connectivity is at acceptable levels.


Aerohive NETWORKS
Supplicant
SW on client dev
Authenticator
Access Point
Authentication
Server (RADIUS)
802.11 association
EAPoL-start
EAP-request/identity
RADIUS-access-request
EAP-response/identity
RADIUS-access-challenge
EAP-request (challenge)
RADIUS-access-request
EAP-response (hashed response)
RADIUS-access-accept (PMK)
Access Granted

Closing thoughts

- Time is money!
- Be conservative.
- Create a lab and break everything.

www.aerohive.com